

# Innspill til personvernstrategi, som del av ny digitaliseringsstrategi

KS er invitert til å gi skriftlig innspill til strategi om personvern knyttet til arbeidet med ny digitaliseringsstrategi. KS har allerede gitt et innspill i flere høringer til strategien. KS sender også inn et overordnet innspill knyttet til de viktigste temaene i strategien for kommunal sektor. I tillegg har KS blitt invitert til å gi forslag til tiltak for styrke personvernet i kommunal sektor særskilt. Offentlig sektors viktigste oppgave er å levere gode, trygge og helhetlige tjenester til innbyggerne. Kommunesektoren er den overlegent største tjenesteleverandøren i offentlig sektor. Kommunal sektor søker en samlet, balansert og helhetlig tilnærming til personvernet som en del av digitaliseringsstrategien.

Innspillet tar utgangspunkt i tre konkrete spørsmål. Dette dokumentet inneholder mulige tiltak KS ønsker å fremme for KDD. Disse tiltakene vil ha stor betydning for å løfte personvern nasjonalt og i kommunesektoren. Noen av tiltakene listes opp gjennomgående i dokumentet sammen med de relevante utfordringene, mens de sentrale og helt avgjørende tiltakene kommer i tabellen på slutten. Ytterligere tiltak kan beskrives nærmere på senere tidspunkt.

## Hva er de største personvernutfordringene innenfor kommunesektoren?

### Utfordringer på samfunnsnivå

På samfunnsnivå gjenspeiles utfordringene i holdninger til personvern der personvern anses som utfordrende å ivareta i et digitalt samfunn. Personvern og informasjonssikkerhet er avgjørende for tillit til informasjonssystemene og felleskomponentene som tas i bruk, men oppleves ofte som en hindring for digitaliseringsprosjekter. Dette kan delvis skyldes mangel på forståelse og et lite tilgjengelig og omfattende personvernregelverket. Strategien må være tydelig på at personvern ikke omtales som et hinder for digitaliseringen.

Personvern og informasjonssikkerhet bør anses som en forutsetning for vellykket digitalisering, og det må være en ambisjon å få til godt personvern samtidig som kommunen kan løse sine oppgaver.

Digitaliseringsstrategien bør også adressere hva slags samfunn vi ønsker oss. Etske problemstillinger bør inngå som en del av personverndiskusjoner i større grad enn i dag. Kommunene må være bevisste på de etiske utfordringene og problemstillingene som oppstår i digitaliseringen, særlig når nye plattformer og nye teknologier tas i bruk.

### Utfordringer med hensyn til prosesser (regelverksutfordringer)

Når det gjelder prosesser, er utfordringene knyttet til regelverkets kompleksitet.

Personvernregelverket er lite tilgjengelig, med uklart nasjonalt handlingsrom og overlappende og delvis rigid sektorregelverk. For å håndtere dette, er det behov for bedre tilgjengelighet av regelverket f.eks. gjennom veiledning og digitalisering av krysshenvisninger for de mest brukte

bestemmelsene i personvernregelverket. Et eksempel på en slik digitalisering er en digital løsning der bestemmelsene i personvernforordningen har henvisninger til relevante bestemmelser i forordningen selv eller til annet regelverk, f. eks informasjonssikkerhetsregelverk.

Datadeling er en viktig forutsetning for digitalisering. En av hovedutfordringene innenfor digitalisering i dag er at det er et gap mellom behov for å dele data og de rammene som personvernregelverket setter gjennom en EU-forordning som ikke kan påvirkes i særlig grad. Det er viktig at regelverk som regulerer personvernet, sees opp mot andre regelverk som regulerer tjenestenes behov for deling av informasjon slik at regelverksfortolkninger ikke står i veien for deling av informasjon som er viktig både for vernet om enkeltmennesket og nytte for samfunnet i stort. Dette understreker viktigheten av arbeidet med nasjonalt handlingsrom og regelverksutvikling som nevnt over.

Det er også viktig at det etableres gode løsninger for at vi som enkeltmennesker i større grad settes i stand til enkelt å kunne regulere og gi samtykke til deling av informasjon om oss selv mellom de som trenger slik tilgang enten for å gjøre jobben sin – eller utvikle tjenester eller kunnskapsutvikling av stor nytte for samfunnet. Det må også etableres gode universelle fullmaktsløsninger slik at vi kan delegerer til andre å ivareta våre behov i bruk av digitale løsninger når vi selv ikke lenger er i stand til det.

Det er flere EU-regelverk som skal spille sammen med personvernregelverket for å lykkes med digitaliseringen. Flere av de nye EU-regelverkene kommer med mange kravsett, og det er ofte uklart hvordan kravene skal forstås og sammenhengen mellom dem, og ikke minst hierarkiet. Her er det behov for samordning.

### Utfordringer knyttet til teknologi

Teknologiske utfordringer omfatter blant annet manglende oppfyllelse av krav til innebygd personvern i mange systemer. Erfaringsmessig blir innebygd personvern forstått for snevert, ofte kun som krav til tilgangsstyring, mens det i realiteten handler om etterlevelse av alle personvernprinsippene. Krav til dataminimering og pseudonymisering er sågar fremhevet i GDPR artikkel 25 om innebygd personvern. Det finnes flere veiledere om hvordan å bygge personvern inn i systemer. Det som trengs, er den systematiske og helhetlige tilnærmingen til anskaffelse og systemutvikling der offentlige virksomheter stiller alle de viktige kravene for å etterleve regelverket.

Videre er manglende oversikt over systemer og utvikling av løsninger uten å ta hensyn til behovet for å bruke data til oppgaveløsning, kvalitetsforbedring og videreutvikling en utfordring. I denne sammenhengen er det viktig å ha fokus på helhetlig informasjonsforvaltning på tvers av forvaltningsnivå, noe som også vil bidra til mer effektiv datadeling og bedre styringsdata. Dette vil føre til økt risikoforståelse og bedre etterlevelse av regelverket.

Det utvikles stadig ny teknologi som utfordrer personvernet. Det er ofte vanskelig å overskue konsekvensene for innbyggernes personvern når ny teknologi skal tas i bruk, f.eks. ved bruk av kunstig intelligens. Det er behov for klare føringer for hvordan teknologi som kunstig intelligens kan brukes på en effektiv og personvernvennlig måte.

## Utfordringer knyttet til menneskelige faktorer

Menneskelige faktorer, spesielt kompetanse, er også kritisk og en forutsetning for å ivareta personvern i digitaliseringen. Det er behov for en felles forståelse av hvordan kravene til personvern skal forstås i praksis. Veiledning og rammeverk kan bidra til å adressere manglende kompetanse. I tillegg er det også behov for økt involvering av innbyggere for god digitalisering. Et eksempel der innbyggerne med fordel kan engasjeres, er utvikling av biblioteker av kategorier av personopplysninger med sensitivitetsgrad som oppslagsverk som kommunene kan benytte seg av. Det vil være tidsbesparende fordi kommunene slipper å gjøre vurderinger av kategorier av personopplysninger hver gang man behandler personopplysninger.

Mange er frustrert over det offentliges manglende evne til samhandling både på nasjonalt og kommunalt nivå. En forbedret samhandling vil føre til mer koordinert og helhetlig tilnærming til personvernet, samt at det vil bidra til at digitaliseringen ses i sammenheng på tvers av alle sektorer.

Her vil videreutvikling av regelverk – i stor grad etablert i en analog tid – og regelverksfortolkning være helt avgjørende. Det er derfor et behov for å styrke arbeidet med de eksisterende samhandlingsarenaene.

## Hvor ser KS en positiv utvikling?

Det er gledelig å se en økning i bevisstheten om og fokuset på personvern i samfunnet generelt og i offentlig sektor spesielt. Personvern og personopplysningssikkerhet er etter hvert blitt en stadig mer naturlig del av arbeidet i digitaliseringsprosjekter, og de fleste organisasjoner rapporterer nå på etterlevelsen av personvernregelverket i sine årsrapporter. Dette har bidratt til å øke toppledelsens eierskap til personvernarbeidet i organisasjonen.

En økt tendens til deling av informasjon om større personvern-avvik har også ført til en bevissthet om risikoen knyttet til mangelfull ivaretagelse av personvernet blant politikere, ledere, medarbeidere og innbyggere generelt. Det er vår oppfatning at det har vært en positiv utvikling i viljen til deling av informasjon og verktøy for personvernarbeid i en rekke organisasjoner, og dette har vært med på å løfte den kollektive forståelsen av både muligheter og utfordringer knyttet til etterlevelsen av personvernregelverket. Personvernverktøy som f.eks. maler for personvernkonsekvensvurderinger, databehandleravtalemaler, praktiske retningslinjer mv. finnes og utvikles i stort omfang og videreutvikles kontinuerlig. Viljen til å dele slike verktøy og samarbeid om bruk blir stadig større.

I sammenhenger der personvernregelverket svært ofte ble omtalt som en hindring for utvikling, er stadig flere blitt oppmerksomme på handlingsrommet som ligger i personvernregelverket og at etterlevelse av regelverket bidrar til bedre digitalisering og ikke det omvendte.

Flere samfunnsaktører bidrar i dag med gode veiledninger om ivaretagelsen av informasjonssikkerhet, personopplysningssikkerhet og personvern. Det er en økning i antall veiledningsaktører som tar personvern med i deres veiledningsaktiviteter, samt at det er stadig mer samarbeid mellom veiledningsaktørene, kommuner og andre offentlige organer. Samordning av aktørene er bra, men det kan fortsatt være vanskelig å orientere seg i "jungelen" av gode veiledere. Denne utfordringen har blitt møtt med et samarbeid mellom aktørene for å samordne veiledningsmaterialet. Nettverk for veiledningsaktører, som ledes og administreres av

Digitaliseringsdirektoratet, er et eksempel på ett tiltak som skal bidra til bedre samordning av veiledningsmaterialet og dermed også en bedre brukeropplevelse for målgruppen veiledningene retter seg mot. Bredden i Nettverk for veiledningsaktører er svært viktig for oversikten over ulike aktiviteter på området, samt at den bidrar til innsikt i behovene til brukerne av veiledningsmaterialet. Andre nettverk og medlemsorganisasjoner bidrar også med målrettet veiledning, erfaringsdeling og utvikling av maler, som bidrar til å forenkle etterlevelsen av personvernregelverket i en rekke organisasjoner. Kommunesektorens organisasjon (KS) bidrar selv gjennom samstyingsstrukturen med fagrådene er med på å løfte kompetansen innen områdene digitalisering, virksomhetsarkitektur, informasjonssikkerhet og personvern i kommunal sektor. Foreningen kommunal informasjonssikkerhet (KINS) er et annet eksempel på en organisasjon som i dag bidrar aktivt og direkte til etterlevelse av krav til informasjonssikkerhet og personvern i kommunal sektor. av medlemmene. I tillegg er det etablert flere velfungerende nettverk, herunder nettverk for personvernombud i kommunal sektor og foreningen personvernombudene som er åpen for både offentlig og privat sektor. Disse nettverkene bidrar til å øke det enkelte personvernombuds kompetanse og derved også bedre veiledning internt i organisasjonene, samt bedre informasjon og veiledning til de registrerte.

Uavhengig av dette, arbeider KS for redusert kompleksitet, og at flere aktører ikke skal ha overlappende veiledningsoppgaver og produkter overfor kommunal sektor. I stort oppfatter vi fortsatt aktørkartet på statlig side som for stort, og at arbeidet i større grad kan konsolideres og overlappende oppgaver og parallelle aktiviteter samordnes. Det ville trolig også være samfunnsøkonomisk lønnsomt, samtidig som at kompetanse det er knapphet på i stort ville kunne utnytted bedre.

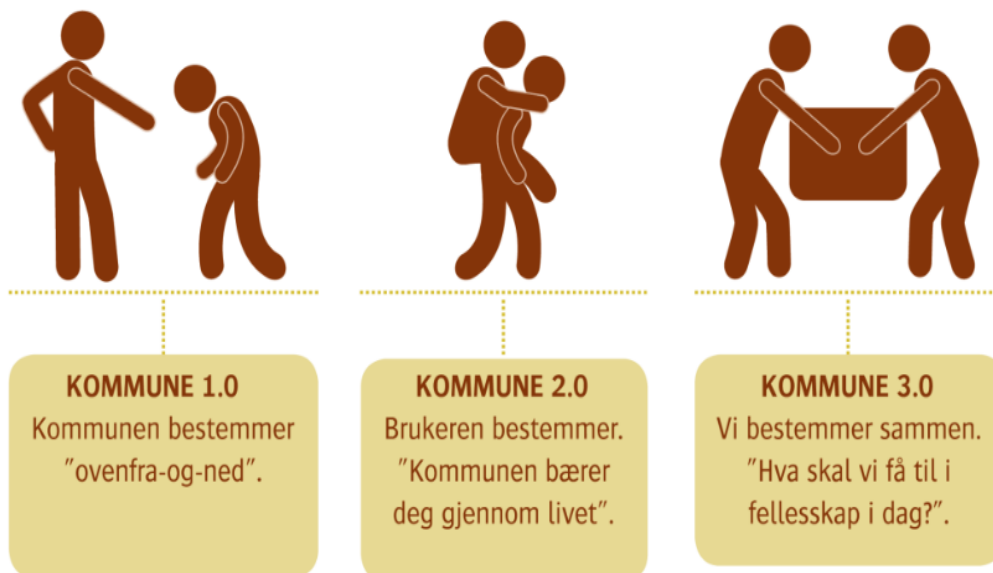
## Hva må en strategi for personvern adressere, og hva kan være aktuelle tiltak?

De største utfordringene knyttet til personvern i digitalisering av kommunale tjenester, er at tjenestene er komplekse og ofte vil involvere ulike sektorer. Dette må tas i betraktning for å sikre en helhetlig tilnærming til personvern. Det vil være nødvendig å analysere målene med digitaliseringen for å identifisere og håndtere disse utfordringene. Dette er en forutsetning for et vellykket samspill mellom personvern og digitalisering. I denne sammenhengen er god informasjonssikkerhet en nødvendig forutsetning for å oppnå et sterkt personvern.

Digitaliseringsstrategien bør inneholde et klart nasjonalt mål bilde for personvern og digitalisering, noe som er viktig for å kunne identifisere konkrete og treffende tiltak. For å nå dette nasjonale målbildet bør man vurdere å etablere en egen handlingsplan for kommunal sektor. En eventuell handlingsplan bør ta inn i seg de ulike tjenesteområdene i en kommune, der det kan være ulike behov knyttet til mål, som igjen kan føre til behov for egne tiltak for de enkelte tjenesteområdene. Dette vil antagelig være et av de viktigste tiltakene for å nå det nasjonale målbildet.

Nedenfor belyses det hva som kan være mål for kommunal sektor i en personvernstrategi, etterfulgt av tre konkrete tiltak som er helt avgjørende for å styrke personvernet nasjonalt men særskilt i kommunal sektor.

Et viktig mål for personvernstrategien bør være å gi innbyggerne mulighet til å styre tilgangen til egne personopplysninger. En tilnærming hvor de som leverer offentlige tjenester bestemmer sammen med dem de leverer tjenester til, finner vi også igjen i Stortingsmelding nr. 47 (2008-2009). Denne inneholdt mål og virkemidler for samskappingsreformen i helse- og omsorgstjenestene. I kjølvannet av meldingen ble det i kommunene satt søkelys på hvordan demografiutvikling, nye styringsreformer og ytre drivkrefter påvirker hvordan kommunen må løse sitt samfunnsoppdrag. En viktig brikke for å løse oppdraget i fremtiden var å dreie tjenestene fra tjenesteorientert til innbyggerorientert. Denne dreiningsprosessen innebærer at innbyggerens selvbestemmelse, selvhjulpenhet og eget ansvar er utgangspunkt for vurdering av behov for kommunens tjenester. Innbyggerens rett til å medvirke er en ressurs og bidrar til kvalitet.



I konseptet kommune 3.0 for samskaping har innbyggerne reell innflytelse på saksbehandlingen og hvordan tjenester tilrettelegges for størst mulig grad av selvhjulpenhet. Dette står i kontrast til visse praksiser som ikke oppfyller kravene til samskaping:

- Når kommunen sender nesten ferdige løsninger på høring, blir samskaping svekket.
- Innbyggere blir involvert i forhåndsprogrammerte prosesser, og politiske beslutninger tas uten å konsultere innbyggerne.
- Kommunikasjonsløsninger som ikke fungerer for hverken innbyggere eller saksbehandlere kan føre til at kommunen fjerner seg fra innbyggerne. Tilbakemelding fra innbyggere viser at kommunikasjonen mellom innbyggere og kommunen ofte føles som i "kommune 1.0," der kommunen oppfattes som en autoritet, og kommunikasjonen er ikke tilrettelagt for en moderne, selvbetjent tilnærming.

En ny digitaliseringsstrategi med personvern og informasjonssikkerhet i bunn, bør ha som mål at ingen innbygger skal ha følelsen av å bo i en kommune 1.0.

Personvernstrategien bør, som i Kommune 3.0, ha en fellesskapstilnærming og peke på hva offentlig sektor kan gjøre i fellesskap for å få til et godt personvern. En slik fellesskapstilnærming ser vi også i Personvernkommisjonens rapport (NOU 2022: 11).

For å lykkes med digitaliseringen i kommunal sektor med et sterkt personvern, må det gjennomføres helhetlige tiltak med fokus på innbyggernes behov og rettigheter. Følgende tre tiltak vil være helt avgjørende i denne sammenhengen.

Nr.	Behov og bakgrunn	Konkrete tiltak
1.	<p>Det er behov for større kompetanse, mer effektiv ressursbruk, felles forståelse og samhandling innenfor kommunesektoren knyttet til personvernarbeid.</p> <p>Dette vil bidra til at alle kommuner går i samme takt og retning.</p>	<p>Vurdere etablering av kommunesektorens kompetansemiljø/senter for personvern.</p> <p>Dette miljøet kan ha ansvar for å koordinere arbeid på tvers av kommunene, og mellom kommunesektoren, næring og statlige organer.</p> <p>Et slikt organ kan f.eks. sørge for koordinert innsats innenfor:</p> <ul style="list-style-type: none"> <li>○ gjennomføring av felles personvernkonsekvensvurderinger for kommunene som kan brukes som utgangspunkt for alle kommunene</li> <li>○ utvikling av felles nasjonale/kommunale personvernverktøy (f. eks. felles malverk, standarder, retningslinjer, veiledninger ol.)</li> <li>○ kunnskapsdeling og målrettede kompetansehevingstiltak</li> <li>○ fortolkning av særlige utfordrende regelverk for kommunesektoren</li> <li>○ veiledningstjenester generelt inkl. veiledning om regelverksanvendelse</li> <li>○ koordinere regelverksutviklingsarbeid for kommunene</li> <li>○ koordinere arbeid med leverandører, f. eks. dialog med store teknologiaktører</li> </ul>

		<p>Et slikt kompetansemiljø/senter vil bidra til effektivt og enhetlig personvernarbeid med høy kvalitet i kommunesektoren.</p> <p>KS vil gjerne ha en nærmere dialog om utforming av et slik tiltak.</p>
<p>2.</p>	<p>Det er behov for koordinert arbeid innenfor regelverksutvikling og en mer harmonisert tilnærming til regelverksanvendelse.</p> <p>Dette er helt sentralt for å få til et samspill mellom digitalisering og personvern og er avgjørende for trygg og lovlig digitalisering.</p>	<ul style="list-style-type: none"> <li>○ Koordinert arbeid for å finne nasjonalt handlingsrom i regelverket</li> </ul> <p>Kommunens oppgaveløsning går på tvers av mange sektorer. En samlet innsats for å finne det faktiske handlingsrommet GDPR legger opp til må gjøres i et konkret kommuneperspektiv, og dette vil bidra til overblikk over helheten og sammenhengen på tvers av lover og forskrifter og på tvers av alle sektorer.</p> <ul style="list-style-type: none"> <li>○ Styrket nasjonalt arbeid med personvernkonsekvensvurderinger knyttet til lovarbeid, ref. GDPR art. 35 nr. 10</li> </ul> <p>En måte å få fart på digitaliseringen på samtidig som man ivaretar personvernet, er å sikre at det gjøres en personvernkonsekvensvurdering (DPIA) i forbindelse med lovarbeid. Da vil man kunne utvikle hjemler som kan gi unntak fra å gjøre DPIA i konkrete tilfeller, noe som vil være svært tidsbesparende i digitaliseringsprosesser.</p> <ul style="list-style-type: none"> <li>○ Samordnet nasjonale tilpasninger i sektorregelverk</li> </ul> <p>Det må sikres at de nasjonale tilpasninger i sektorregelverket er i tråd med personvernregelverket og faktisk kan gjennomføres i praksis for å sikre en mer effektiv digitalisering.</p> <ul style="list-style-type: none"> <li>○ Samordnet nasjonale tilpasninger av EU regelverk knyttet til digitalisering og digital sikkerhet</li> </ul> <p>Det er også behov for samordning mellom personvernregelverk og de</p>

		<p>andre regelverkene, særlig regelverk som angår informasjonssikkerhet (f. eks. ny lov om digital sikkerhet og andre regelverk fra EU på området digital sikkerhet) og ny teknologi som kunstig intelligens. Det bør gjøres et koordinert arbeid nasjonalt (på departements- og direktoratsnivå) for å tegne et tydelig rettskildebilde som kan brukes i praksis i tillegg til en tydeliggjøring av konsekvenser av de ulike regelverkene.</p> <p>Det ovennevnte kommunesektorens kompetansemiljø/senter for personvern kan evt. delta i slikt arbeid på vegne av kommunene.</p>
<p>3.</p>	<p>Det er behov for å løfte personvern til politisk nivå.</p> <p>Et av de mest fremtredende tiltakene foreslått av Personvernkomisjonens rapport (NOU 2022: 11) er forslaget om at det etableres en nasjonal personvernpolitikk, "som legger føringer for digitaliseringen av samfunnet i tillegg til hva som følger av lovgivningen" (pkt. 1.2).</p> <p>KS støtter at personvernstrategi blir en del av ny digitaliseringsstrategi for å kunne få til en nasjonal personvernpolitikk.</p>	<ul style="list-style-type: none"> <li>○ Felles føringer for kommunene om at enhver kommune skal som minimum sikre at personvern løftes til politisk ledelse årlig. Dette er i tråd med Personvernkomisjonens rapport, som foreslår at regjeringen årlig bør legge frem en personvernpolitisk redegjørelse for Stortinget.</li> <li>○ Målrettet kompetansetiltak mot folkevalgte for å få personvern høyere opp på den politiske agendaen.</li> </ul>